In the Specification:

Rewrite the paragraph at page 1, lines 19-21, as follows:

The present invention relates to wireless communication systems, such as cellular systems and PCS systems, and more particularly relates to methods ~~and systems for reducing theft of wireless telephony services by~~ **involving** use of steganographically encoded ~~authentication~~ data **in conjunction with such systems**.

Rewrite the paragraph at page 3, lines 7-12, as follows:

To overcome this failing, ~~the preferred embodiments of the present invention~~ **one embodiment** steganographically encodes the voice signal with identification data, resulting in "in-band" signaling (in-band both temporally and spectrally). This approach allows the carrier to monitor the user's voice signal and decode the identification data therefrom.

Rewrite the paragraph extending between page 3, line 18 and page 4, line 5, as follows:

In ~~the preferred form of the invention~~ **certain embodiments**, the steganographic encoding relies on a pseudo random data signal to transform the message or identification data into a low level noise-like signal superimposed on the subscriber's digitized voice signal. This pseudo random data signal is known, or knowable, to both the subscriber's telephone (for encoding) and to the cellular carrier (for decoding). Many such embodiments rely on a deterministic pseudo random number generator seeded with a datum known to both the telephone and the carrier. In simple embodiments this seed can remain constant from one call to the next (e.g. a telephone ID number). In more complex embodiments, a pseudo-one-time pad system may be used, wherein a new seed is used for each session (i.e. telephone call). In a hybrid system, the telephone and cellular carrier each have a reference noise key (e.g. 10,000 bits) from which the telephone selects a field of bits, such as 50 bits beginning at a randomly selected offset, and each uses this excerpt as the seed to generate the pseudo random data for encoding. Data

sent from the telephone to the carrier (e.g. the offset) during call set-up allows the carrier to reconstruct the same pseudo random data for use in decoding. Yet further improvements can be derived by borrowing basic techniques from the art of cryptographic communications and applying them to the steganographically encoded signal detailed in this disclosure.

Rewrite the paragraph at page 5, lines 10-12, as follows:

Walter Bender at M.I.T. has done a variety of work in the field, as ~~illustrate~~ **illustrated** by his paper "Techniques for Data Hiding," Massachusetts Institute of Technology, Media Laboratory, January 1995.

Rewrite the paragraph at page 6, lines 4-6, as follows:

The foregoing and additional features and advantages of **certain embodiments of** the present invention will be more readily apparent from the following detailed description, which proceeds with reference to the accompanying drawings.

Rewrite the paragraph at page 7, lines 6-13, as follows:

The process works in reverse when receiving. A broadcast from the cell **[[cite]]** **site** is received through the antenna 26. RF section 24 amplifies and translates the received signal to a different frequency for demodulation. Demodulator 28 processes the amplitude and/or phase variations of the signal provided by the RF section to produce a digital data stream corresponding thereto. The data unformatter 30 segregates the voice data from the associated synchronization/control data, and passes the voice data to the D/A converter for conversion into analog form. The output from the D/A converter drives the speaker 34, through which the subscriber hears the other party's voice.

Rewrite the paragraph at page 8, lines 1-11 as follows:

The illustrated encoder 36 operates on digitized voice data, auxiliary data, and pseudo-random noise (PRN) data. The digitized voice data is applied at a port 40 and is provided, e.g., from A/D converter 18. The digitized voice may comprise 8-bit samples. The auxiliary data is applied at a port 42 and comprises, in one form of the invention, a stream of binary data uniquely identifying the telephone 10. (The auxiliary data may additionally include administrative data of the sort conventionally exchanged with a cell site at call set-up.) The pseudo-random noise data is applied at a port 44 and can be, e.g., a signal that randomly alternates between "-1" and "1" values. (More and more cellular phones are incorporating spread spectrum capable circuitry, and this pseudo-random noise signal and other aspects of this invention can often ~~Apiggy-back~~ **"piggy back"** or share the circuitry which is already being applied in the basic operation of a cellular unit).

Rewrite the paragraph extending between page 14, line 27 and page 15, line 20, as follows:

The continued and inevitable engineering improvement in the detection of embedded code signals will undoubtedly borrow heavily from this generic field of known signal detection. A common and well-known technique in this field is the so-called "matched filter," which is incidentally discussed early in section 2 of the Kassam book. Many basic texts on signal processing include discussions on this method of signal detection. This is also known in some fields as correlation detection. Where, as here, the location of the auxiliary signal is known a priori (or more accurately, known to fall within one of a few discrete locations, as discussed above), then the matched filter can often be reduced to a simple vector dot product between a set of sparse PRN data, and mean-removed excerpts of the composite signal corresponding thereto. (Note that the PRN data need not be sparse and may arrive in contiguous bursts, such as in British patent publication 2,196,167 mentioned earlier wherein a given bit in a message has contiguous PRN

values associated with it.) Such a process steps through all 480 sparse sets of PRN data and performs corresponding dot product operations. If the dot product is positive, the corresponding bit of the auxiliary data signal is a "1;" if the dot product is negative, the corresponding bit of the auxiliary data signal is a "0." If several alignments of the auxiliary data signal within the framed composite signal are possible, this procedure is repeated at each candidate alignment, and the one yielding the highest correlation is taken as true. (Once the correct alignment is determined for a single bit of the auxiliary data signal, the alignment of all the other bits can be determined therefrom. ~~A Alignment, perhaps better known as Asynchronization,~~ **"Alignment," perhaps better known as "synchronization,"** can be achieved by primarily through the very same mechanisms which lock on and track the voice signal itself and allow for the basic functioning of the cellular unit).

Rewrite the paragraph at page 16, lines 17-19, as follows:

Security ~~of the present invention~~ depends, in large part, on security of the PRN data and/or security of the auxiliary data. In the following discussion, a few of many possible techniques for assuring the security of these data are discussed.

Rewrite the paragraph extending between page 18, line 19 and page 19, line 7, as follows:

In this embodiment, a ROM in the telephone stores 256 different messages (each message may be, e.g., 128 bits in length). When the telephone is operated to initiate a call, the telephone randomly generates a number between 1 and 256, which serves as an index to these stored messages. This index is transmitted to the cell site during call set-up, allowing the central station to identify the expected message from a matching database on secure disk 52 containing the same 256 messages. (Each telephone has a different collection of messages.) (Alternatively, the carrier may randomly select the index number during call set-up and transmit it to the telephone, identifying the message to be used during that session.) In a theoretically pure world where proposed attacks to a secure system are only mathematical in nature, much of these additional layers of security might

seem superfluous. (The addition of these extra layers of security, such as differing the messages themselves, simply acknowledge that the designer of actual public-functioning secure systems will face certain implementation economics which might compromise the mathematical security of ~~the core principals of this invention~~ **underlying principles of such embodiments**, and thus these auxiliary layers of security may afford new tools against the inevitable attacks on implementation).

Rewrite the paragraph at page 20, lines 1-5, as follows

Since the ~~preferred embodiments of the present invention~~ **illustrative embodiments** each redundantly encodes the auxiliary data throughout the duration of the subscriber's digitized voice, the auxiliary data can be decoded from any brief sample of received audio. In ~~the preferred forms of the invention~~ **such embodiments**, the carrier repeatedly checks the steganographically encoded auxiliary data (e.g. every 10 seconds, or at random intervals) to assure that it continues to have the expected attributes.

Rewrite the paragraph at page 20, lines 17-26, as follows:

While the foregoing discussion has focused on steganographic encoding of the baseband digitized voice data, artisans will recognize that intermediate frequency signals (whether analog or digital) can likewise be steganographically encoded in accordance with principles ~~of the invention~~ **detailed herein**. An advantage of post-baseband encoding is that the bandwidth of these intermediate signals is relatively large compared with the baseband signal, allowing more auxiliary data to be encoded therein, or allowing a fixed amount of auxiliary data to be repeated more frequently during transmission. (If steganographic encoding of an intermediate signal is employed, care should be taken that the perturbations introduced by the encoding are not so large as to interfere with reliable transmission of the administrative data, taking into account any error correcting facilities supported by the packet format).

Rewrite the paragraphs at page 21, lines 11-20, as follows:

As noted earlier, the principles ~~of the invention~~ **detailed herein** are not restricted to use with the particular forms of steganographic encoding detailed above. Indeed, any steganographic encoding technique previously known, or hereafter invented, can be used in the fashion detailed above to enhance the security or functionality of cellular (or other wireless, e.g. PCS) communications systems. Likewise, these principles are not restricted to wireless telephones; any wireless transmission may be provided with an "in-band" channel of this type.

It will be recognized that systems for implementing ~~applicant's invention~~ **the detailed embodiments** can comprises dedicated hardware circuit elements, but more commonly comprise suitably programmed microprocessors with associated RAM and ROM memory (e.g. one such system in each of the telephone 10, cell-site 12, and central office 14).

Rewrite the paragraph at page 22, lines 5-8, as follows:

While the Exhibit B software is particularly designed for the steganographic encoding and decoding of auxiliary data in/from two-dimensional image data, many principles thereof are applicable to the encoding of digitized audio~~, as contemplated by the presently claimed invention~~.